

## A B S T R A C T

## ZERO-KNOWLEDGE PROOF CRYPTOGRAPHIC METHODS AND DEVICES

5       The invention relates to a cryptography method  
 involving a keyholder having a number  $m \geq 1$  of private  
 keys  $Q_1, Q_2, \dots, Q_m$  and respective public keys  $G_1, G_2, \dots, G_m$ , each  
 pair of keys  $(Q_i, G_i)$  (where  $i=1, \dots, m$ ) satisfying either the  
 relationship  $G_i = Q_i^v \bmod n$  or the relationship  $G_i \times Q_i^v = 1 \bmod n$ ,  
 10       where  $n$  is a public integer equal to the product of  $f$   
 (where  $f > 1$ ) private prime factors  $p_1, \dots, p_f$ , at least two  
 of which are separate, and the exponent  $v$  is a public  
 integer equal to a power of 2. The invention teaches  
 among other things what mathematical structure may be  
 15       imparted to the public keys for it to be impossible to  
 calculate said private keys from said public parameters  
 in a reasonable time unless said prime factors are known.  
 The invention also relates to devices adapted to  
 implement the method.

20

25

30

35       Translation of the title and the abstract as they were when originally filed by the  
 Applicant. No account has been taken of any changes that may have been made  
 subsequently by the PCT Authorities acting ex officio, e.g. under PCT Rules 37.2,  
 38.2, and/or 48.3.